

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 03/10015

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/30 H04L9/32 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 61918 A (SILVERBROOK RES PTY LTD ;WALMSLEY SIMON ROBERT (AU); LAPSTUN PAUL) 23 August 2001 (2001-08-23) page 20, line 24 -page 24, line 31	1,3,6, 12,14,15
Y	page 68, line 15 -page 69, line 13 ---	8,10
Y	US 5 991 415 A (SHAMIR ADI) 23 November 1999 (1999-11-23) cited in the application column 1, line 5 -column 2, line 9 column 4, line 12 - line 59 column 6, line 17 - line 52 ---	8,10
	-/--	



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

\* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*&\* document member of the same patent family

Date of the actual completion of the international search

27 January 2004

Date of mailing of the international search report

03/02/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Liebhardt, I

# INTERNATIONAL SEARCH REPORT

International Application No.

PCT/EP 03/10015

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>BONEH D ET AL: "On the importance of checking cryptographic protocols for faults"</p> <p>1997 , ADVANCES IN CRYPTOLOGY- EUROCRYPT. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, SPRINGER VERLAG, DE, PAGE(S) 37-51</p> <p>XP002202745</p> <p>page 49, line 28 - line 30</p> <p>page 50, line 13 - line 14</p> <p>-----</p>	1-15

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 03/10015

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0161918	A	23-08-2001	WO 0161918 A1	23-08-2001
			AU 3144301 A	27-08-2001
			CA 2400223 A1	23-08-2001
			EP 1260054 A1	27-11-2002
			US 2003159036 A1	21-08-2003
US 5991415	A	23-11-1999	AU 7568598 A	08-12-1998
			EP 0986873 A1	22-03-2000
			IL 132816 A	29-05-2003
			WO 9852319 A1	19-11-1998

# INTERNATIONALE RECHERCHENBERICHT

Internationale Patentzeichen

PCT/EP 03/10015

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES  
IPK 7 H04L9/30 H04L9/32 G06F7/72

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 H04L G07F G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, PAJ, INSPEC

## C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 01 61918 A (SILVERBROOK RES PTY LTD ;WALMSLEY SIMON ROBERT (AU); LAPSTUN PAUL) 23. August 2001 (2001-08-23) Seite 20, Zeile 24 -Seite 24, Zeile 31 Seite 68, Zeile 15 -Seite 69, Zeile 13	1,3,6, 12,14,15
Y	-----	8,10
Y	US 5 991 415 A (SHAMIR ADI) 23. November 1999 (1999-11-23) in der Anmeldung erwähnt Spalte 1, Zeile 5 -Spalte 2, Zeile 9 Spalte 4, Zeile 12 - Zeile 59 Spalte 6, Zeile 17 - Zeile 52 ----- -/-	8,10

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

'A' Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

'E' älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

'L' Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

'O' Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

'P' Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

'T' Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

'X' Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

'Y' Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

'&' Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

27. Januar 2004

Absenddatum des internationalen Recherchenberichts

03/02/2004

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+31-70) 340-3016

Bevollmächtigter Bediensteter

Liebhardt, I

## C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	<p>BONEH D ET AL: "On the importance of checking cryptographic protocols for faults" 1997 , ADVANCES IN CRYPTOLOGY- EUROCRYPT. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, SPRINGER VERLAG, DE, PAGE(S) 37-51 XP002202745 Seite 49, Zeile 28 - Zeile 30 Seite 50, Zeile 13 - Zeile 14 -----</p>	1-15

# INTERNATIONALER RESEARCHENBERICHT

Angaben zu Veröffentlichungen, die zu selben Patentfamilie gehören

Internationales Zeichen

PCT/EP 03/10015

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 0161918 A	23-08-2001	WO 0161918 A1	23-08-2001
		AU 3144301 A	27-08-2001
		CA 2400223 A1	23-08-2001
		EP 1260054 A1	27-11-2002
		US 2003159036 A1	21-08-2003
US 5991415 A	23-11-1999	AU 7568598 A	08-12-1998
		EP 0986873 A1	22-03-2000
		IL 132816 A	29-05-2003
		WO 9852319 A1	19-11-1998